METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER WITH SECURE KEY DISTRIBUTION

ABSTRACT

A method and system for securely decrypting and decoding a digital signal is disclosed. One embodiment of the present invention first accesses an encrypted signal at a first logical circuit. Next, this embodiment determines a broadcast encryption key for the encrypted signal at a second logical circuit separate from the first logical circuit. For example, the second logical circuit where the broadcast key was determined may be across a communication link from the first circuit where the signal is being received. Then, the broadcast encryption key is encrypted by means of a public key and transferred over the communication link. Next, at the first logical circuit, the encrypted broadcast encryption key is decrypted. Therefore, the broadcast encryption key is determined. Then, at the first logical circuit, the encrypted signal is decrypted using the broadcast encryption key. Consequently, the encrypted signal is decrypted without exposing the broadcast encryption key on the communication link in an un-encrypted form.